What malicious code is designed to spread through IoT devices?

Mirai is a malicious code designed to spread through IoT devices. Click to see this article now to learn how to prevent your computer from being infiltrated by malicious codes!

Attacks from IoT devices are one of the new forms of network attacks with a very large scale. So do you know which malicious code is designed to spread through IoT devices? Follow this article to better understand as well as know some solutions when encountering this problem.

Question : What malicious code is designed to spread through IoT devices?

Answer : **Mirai** is a malicious code designed to spread through IoT devices. Easily infect devices such as: Security cameras, Routers, printers,. And it can attack the computer 's denial of service .

IoT is being used a lot in the market today, but it is threatened by malicious code, invasive as well as affecting devices. Follow along with the article below to learn more about IoT as well as the types of malicious code that compromise it!

1. What is IoT?

IoT (Internet of Things) is a collection of devices that are able to connect with each other, with the Internet and with the outside world to do a certain job. It is a system of interrelated computing devices, mechanical and digital machines or humans and the ability to transmit data over a network without requiring human-computer interaction.

2. What types of malware are designed to spread through IoT devices?

One of the types of malicious code designed to spread through **IoT** devices that attracts the attention of the public today is the **Mirai** variant **.** This type of malicious code attack has caused many losses to users, especially it can steal personal information as well as important data of users. The most intense attack was in 2017, about 15 million computers were infected with viruses caused by Mirai.

3. Why is USB the main cause of malicious code spreading through IoT devices?

In 2017, about 15 million computers were infected with viruses caused by Mirai, experts analyze the cause of malicious code spreading through IoT devices is due to **USB** . Although USB is a popular means of backing up and exchanging data between computers, the sense of safe use of USB has not been improved much.

How to fix

To limit the spread of viruses through USB, you should download Virus scanning software so that you can scan USB before using or on strange devices. Enterprises should strengthen the solution to control the synchronous security policy to minimize the penetration of malicious code.

4. Type of attack targeting IoT Smarthome

Man-in-the-middle

An attacker disrupts or tamperes with communication between two systems.

Example : Fake temperature data is generated by environmental monitoring devices, creating a spoofing effect and forwarding to the cloud.

Data and identity theft

Data generated by unprotected smart devices will have personal information stolen for transactions for fraud and identity theft.

Device hijacking

An attacker can take control and control the device in a powerful way. These types of attacks are often difficult to detect because their functions do not change too much. As well as very simple operation, only one device is capable of re-infecting other devices in the house.

Distributed Denial of Service (DDoS)

This means that an attacker will find a way to temporarily or indefinitely disrupt the services of an Internet-connected server. The high-traffic, distributed service attack case makes it difficult to prevent cyberattacks by blocking only a single source.

Example : When a sensor is compromised on a network it can infect similar devices running the same software. These infected devices often have to run into the vast army of Botnets to carry out attacks.

Perpetual Denial of Service (PDoS)

This is an attack that damages devices to the point of requiring hardware replacement or reinstallation.

Example : BrickerBot is encrypted to exploit hard-coded passwords in IoT devices and cause a permanent denial of service.

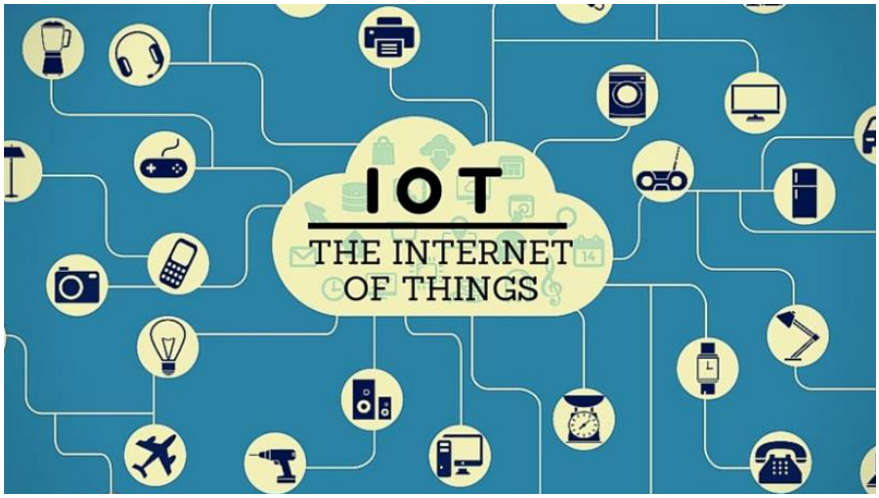
5. How to protect IoT devices from malware

Choose a reliable IoT product

This is the most important thing when using IoT. An IoT device from a reputable supplier will have very strong and safe security equipment. Therefore, in the process of using malicious code is also more limited. Even hackers who want to break into IoT cannot.

Use strong authentication credentials

Most IoT devices will come with factory default passwords. Taking advantage of that opportunity, the hackers broke into the devices with the same default password. Therefore, users need to change the password so that it has high security to keep it out of the eyes of hackers.



Keep IoT devices up to date

New versions come out with the completion of the old version's vulnerabilities. Therefore, it is recommended to update IoT devices regularly to enhance security and safety. All operating systems, management programs, driver programs, etc. need to be updated to the latest version.

6. Signs that IoT devices have been infected with malicious code

Computer/laptop

This is a tool that hackers use to accomplish their goals.

- **Sign**

+ Unusually slow network access, strange toolbar appears.

+ Your account's password is suddenly changed, or you receive fake emails or messages from your account.

+ The computer automatically installs strange software, the mouse pointer runs around and stops at the target specified by the hacker.

+ Anti-virus program, Task Manager, Registry Editor are disabled.

- **How to fix**

Use anti-virus software.

+ Should use genuine software, limit the use of crack tools.

+ Update new versions regularly.

Mobile phone

This is the second device after the computer that hackers keep an eye on.

- **Sign**

+ Heavy loss of battery. If the battery drains unexpectedly quickly, the phone may be infected with malicious code.

+ Phone works slow due to virus attack.

+ The phone is off for a long time, the call is often blocked.

- **How to fix**

+ Need to install anti-virus software for the phone.

+ Be careful when downloading applications, should download high-quality applications.

+ Update new versions regularly.

Other IoT Devices

- **Smart home**

Having hijacked Smartphone, hackers use Smartphone to unlock the house and proceed to infiltrate.

- **Smart car**

A car with an Internet connection can easily and completely control this car after being infiltrated. Hackers can adjust the air conditioning system, radio, can automatically turn off the engine when the car is running, and can even disable the car's brake pedal.

- **Smart locks**

Can be hijacked via Smartphone, hackers can unlock via Wifi, Bluetooth, .

- **Cameras, smart power sockets, TVs with WiFi, bicycles with Bluetooth** : these devices are also easily hacked by hackers if there is no security.

This article has helped you understand what IoT is? And what malicious code spreads through IoT. Hope this article will help you. See you in the next post!